Appendix B: Compliance Checklists

COE compliance is the cornerstone to ensure seamless segment integration and proper system operation. An objective technique for measuring COE compliance is required. Such a system has the following advantages:

¥ it allows quantitative statements to be made about whether or not a segment is compliant,

¥ it provides an objective measure of the degree to which a segment is compliant,

¥ it serves to identify areas in which segments need to improve to achieve compliance, and

¥ it aids it developing a migration strategy for legacy systems.

Chapter 2 defines Category 1 compliance as eight levels of progressively deeper integration, because compliance can not be an all or nothing proposition for legacy systems. The levels progress from a state of "peaceful coexistence" to "federation of systems" to true integration. The philosophy is to begin with an agreement on a set of standards, ensure non-interference when installed on the same LAN, then non-interference when installed on the same workstation, and finally to interoperability through sharing the same software and data. With this strategy, it is possible to define a minimally acceptable level of compliance which balances system risk against cost to achieve full compliance.

This appendix presents a series of checklist items organized by compliance level. It addresses only Category 1 compliance. Segments shall be evaluated against these checklists to determine the degree of compliance. Each item shall be answered as *True*, *False*, or *Not Applicable* as appropriate. The Category 1 compliance level assigned to the segment is the highest numbered level for which there are no "False" replies.

Segments shall achieve Level 7 compliance before being accepted or advertised as an approved DISA product. At DISA's discretion, segments that are Level 5 or Level 6 compliant may be accepted as prototypes and fielded at selected sites for evaluation purposes. Developers must achieve Level 4 compliance before DISA will consider evaluating a prototype for eventual migration into the COE or COE-based DISA systems.

B.1 Standards Compliance (Level 1)

Operating System

T   F   N/A   1.   The operating system is POSIX compliant.

T   F   N/A   2.   If Unix, the operating system is System V.

Network

T   F   N/A   1.   The operating system supports DCE.

T   F   N/A   2.   The operating system supports TCP/IP protocols.

T   F   N/A   3.   The operating system supports udp broadcasts as
                                          well as point to point communications.

T   F   N/A   4.   The operating system supports SLIP and PPP.

Windowing Environment

T   F   N/A   1.   If Unix based, the application is compatible with
                                          X Windows.

T   F   N/A   2.   If X Windows based, the application is Motif
                                          compliant.

Miscellaneous

T   F   N/A   1.   If an RDBMS is used, it supports FIPS-127 SQL
                                          queries.

B.2 Network Compliance (Level 2)

Operating System

**T F   N/A   **1.   The operating system supports NFS, and such usage does not pose additional security risks.

**T F   N/A   **2.   The application is able to operate correctly with the operating system security modules enabled.

Network

**T F   N/A   **1.   The operating system supports Berkeley sockets.

**T F   N/A   **2.   The application is able to operate in a DNS/NIS+ environment.

**T F   N/A   **3.   The application is able to operate in an environment utilizing udp broadcasts as well as point to point tcp connections.

**T F   N/A   **4.   The application does not require any special hostname conventions or have reserved IP addresses.

**T F   N/A   **5.   The application is able to operating correctly on Class B and Class C LANs.

Windowing Environment

**T F   N/A   **1.   If the application resides on a machine with an X server, the X server is compatible with the version in use by the COE.

Database

**T F   N/A   **1.   Database updates operate correctly with DBMS security audits enabled.

**T F   N/A   **2.   The database is recoverable to a consistent state in the event of DBMS server, network or client application failure. This includes both hardware and software failures.

**T F   N/A   **3.   Database transactions implement strict two-phase locking.

B.3 Workstation Compliance (Level 3)

Operating System

T F   N/A   1.   The operating system configuration required by the application does not decrease or conflict with any system resources (shared memory, number of semaphores, etc.) as already configured for the COE.

T F   N/A   2.   The application does not use hardcoded port assignments (e.g., from `/etc/services`) and is not sensitive to specific ports other than well known port assignments (e.g., ftp, listen).

Network

T F   N/A   1.   The application can operate in an environment configured to only use anonymous ftp.

Windowing Environment

T F   N/A   1.   The application can operate on a COE-configured workstation without altering the location or version of any system software (Unix, X Windows, Motif, etc.).

T F   N/A   2.   The application, if using X, does not make direct calls to X libraries that conflict with Motif.

T F   N/A   3.   The application does not alter any files in the vendor supplied X or Motif directories (e.g., modify `rgb.txt` or `Xdefaults`) unless authorized by the DISA Chief Engineer.

T F   N/A   4.   The application can use the same X server version and `xdm` version that the COE uses.

T F   N/A   5.   The application, if using Motif, can either use the same version as the COE, or does a static link to Motif libraries so that it does not conflict with other COE-based segments.

Database

T   F   N/A   1.   The application does not modify the user's DBMS
environment.

COTS Products

T F   N/A   1.   The software is capable of running in an environment that includes COE procured COTS products (Gain Momentum, Sybase®, Oracle®, Applix, etc.).

T F   N/A   2.   Configuration changes made to COTS products, if any, do not render inoperable any COE-based segment.

T F   N/A   3.   The application does not require any source code modifications to COTS products, except as authorized by the DISA Chief Engineer. (Some commercial products, such as `xdm`, may require modification for security reasons. The application must work with `xdm` as provided by the COE.)

Miscellaneous

T F   N/A   1.   The software does not alter any files outside its own directory in a way that conflicts with any other COE-based segment.

B.4 Bootstrap Compliance (Level 4)

Security

T F N/A   1.   If an aggregate, the security level of the parent dominates the security level of the children.

T F N/A   2.   Documentation is submitted with the segment that clearly identifies releasability restrictions.

Standards Compliance

T F N/A   1.   All software and data are in segment format.

T F N/A   2.   The segment successfully passes `VerifySeg` with no errors.

T F N/A   3.   The segment uses the same bootstrap COE as the target COE-based system (e.g., GCCS, GCSS).

T F N/A   4.   The segment can be installed and removed through the COE installation tools.

Database

T F N/A   1.   Owners do not use system storage areas during database creation.

T F N/A   2.   The segment does not modify the core database storage areas, create objects in system storage areas, or create objects in public storage areas.

COTS Products

T F N/A   1.   The segment uses the same COTS configurations as the COE-based target system for any other COTS product that may also reside on the workstation.

Runtime Environment

**T F   N/A   1.   The segment uses the same runtime environment
configuration as the COE-based target system with
extensions, if any, made through environment
extension files and segment descriptors.

**T F   N/A   2.   The segment uses the same versions, configurations,
and file locations as the COE for all components of
the bootstrap COE.

B.5 Minimal COE Compliance (Level 5)

Security

T F   N/A   1.   The segment does not alter the COE established
`umask` setting.

T F   N/A   2.   Prior approval has been granted by the DISA Chief
Engineer to provide a command line mode or feature.

Standards Compliance

T F   N/A   1.   The segment uses the same kernel COE as the target
COE-based system.

T F   N/A   2.   All directory and file names contain only printable,
non-blank characters.

T F   N/A   3.   The segment does not create user login accounts.
(This does not apply to the account group segments
which are part of the kernel COE.)

T F   N/A   4.   The segment can operate in an environment where
user accounts are created and deleted without notice.
The segment accounts for this and creates and
initializes operator preferences the first time the
segment is activated after a new account is created.

T F   N/A   5.   The segment does not require being loaded in any
specific directory, or a waiver has been granted by
the DISA Chief Engineer. (This requirement does not
apply to COTS segments.)

T F   N/A   6.   The segment conforms to the COE version numbering
scheme.

Operating System

T F   N/A   1.   The segment does not rename well defined ports
(e.g., ftp, listen), or declare new port names which
have the same port number as well defined ports in
the `/etc/services` file.

Windowing Environment

T F   N/A   1.   The segment is Motif compliant and can use `mwm` as the window manager.

T F   N/A   2.   The segment is compatible with the `XFONTSDIR`, `XAPPLRESDIR`, and `XENVIRONMENT` settings established by the COE.

Database

T F   N/A   1.   The database segment is separate from the application segment.

T F   N/A   2.   Applications are not required to be on the database server to operate correctly.

T F   N/A   3.   Users are not tied to a particular server.

T F   N/A   4.   The segment installation revokes the owner account's DBMS login privilege upon successful completion of database installation.

T F   N/A   5   Definitions of schema components are provided in the DBMS data dictionary.

T F   N/A   6.   Segment dependencies (if any) are documented in the `Requires` file of the `SegDescrip` directory. Separate segments must be provided that create required database dependencies. These segments are executed by the owning database(s).

T F   N/A   7.   The owner accounts are not used to connect to databases.

T F   N/A   8.   Owners do not have database administrator privileges.

T F   N/A   9.   The segment installation requires the database administrator to change the password of the owner account upon completion.

T F   N/A   10.   The core DBMS instance's configuration is used.

T F N/A 11. The segment does not assume any particular disk configuration when creating data files. The segment creates all data files in the `DBS_files` subdirectory.

T F N/A 12. Any modified versions of DBMS COE tools reside with the application's client segment.

T F N/A 13. Scripts are provided for the DBA's use to add, modify and remove users privileges.

T F N/A 14. The segment does not modify the another segment's database schema.

T F N/A 15. Grants are not made to general purpose users (e.g. Oracle's PUBLIC user).

T F N/A 16. Only the owner or the DBA are able to administer grants.

T F N/A 17. The application does not set or redirect the users' DBMS connection (e.g., Oracle's `TWO_TASK` variable).

T F N/A 18. The database server segment is removable (e.g., has a `DEINSTALL` capability).

T F N/A 19. Database constraints are in scripts that are separate from those used to create data objects.

T F N/A 20. The application database server segment provides a non-destructive update/reload capability.

Runtime Environment

T F N/A 1. The segment is launched from the same desktop provided with the COE.

T F N/A 2. The segment uses relative pathnames for files within the segment.

T F N/A 3. The segment home environment variables points to the segment's home directory.

T F N/A 4. The segment does not use the "~" character for referencing pathnames in environment extension files

which become a part of the global runtime environment.

T F N/A 5. The segment does not use any reserved symbols as its own from Chapter 5 unless authorized to do so by the DISA Chief Engineer.

T F N/A 6. The segment does not override or alter any environment variable that it doesn't create.

T F N/A 7. The segment completely separates the development environment from the runtime environment, and no development environment tools, scripts, or other executables are required at runtime.

T F N/A 8. The segment does not alter any environment variables set by the affected account group except through environment extension files.

COE Component Segments

T F N/A 1. The segment has been authorized as a COE component segment by the DISA Chief Engineer.

T F N/A 2. COE component segments in the kernel COE fully specify dependencies upon the components in the bootstrap COE.

T F N/A 3. If a parent COE component segment, the following environment variables are automatically defined as specified by this document:

```
DATA_DIR
LD_LIBRARY_PATH
LOGNAME
LOG_NAME
LOGIN_NAME
MACHINE
MACHINE_CPU
MACHINE_OS
path
TMPDIR
TZ
XAPPLRESDIR
XFONTSDIR
XENVIRONMENT
```

T F N/A   4.   If a COE component segment, the segment does not alter the `path` environment variable. (This rule does not apply to the parent COE component segment.)

T F N/A   5.   If a COE component segment, all executables use the segment prefix unless otherwise approved by the DISA Chief Engineer. (Certain segments may be "grandfathered" by the Chief Engineer.)

T F N/A   6.   If a COE component segment, all environment variables are named with the segment prefix unless otherwise approved by the DISA Chief Engineer. (Certain segments may be "grandfathered" by the Chief Engineer.)

Account Groups

T F N/A   1.   If an account group segment, prior approval has been received from the DISA Chief Engineer to create an account group segment.

T F N/A   2.   If an account group segment, the environment settings from `/h/COE/Scripts` are automatically included.

T F N/A   3.   If an account group segment, the segment provides files of the form `filename.segprefix` for all environment files that segments may reference or extend through the `ReqrdScripts` descriptor.

T F N/A   4.   If an account group segment, the segment provides an executable in the `Scripts` subdirectory, named `Runxxx` where `xxx` is the segment prefix, to initiate execution of the account group's application.

T F N/A   5.   If an account group segment, the following environment variables are defined:

```
COE_SYS_NAME
DISPLAY
HOME
path
SHELL
TERM
```

```
USER
USER_HOME
USER_DATA
USER_PROFILE
```

Aggregate Segments

T   F   N/A   1.   If an aggregate child segment, the segment does not specify a dependency on other children in the aggregate, nor on the parent.

T   F   N/A   2.   If an aggregate parent segment, the segment does not specify a dependency on any of its child segments.

Segment Descriptors

T   F   N/A   1.   The segment uses `SegInfo` or individual segment descriptor files, but not both.

T   F   N/A   2.   The segment describes all background processes, if any, through the `Processes` descriptor.

T   F   N/A   3.   All segment dependencies and conflicts are fully declared through the appropriate descriptor. (Mission application segments need not specify dependencies on segments contained in the kernel COE unless they are version sensitive. COE component segments need not specify dependencies on the kernel COE unless they are sensitive to version changes in the kernel COE.)

T   F   N/A   4.   Memory and disk space requirements are fully and accurately specified in the `Hardware` descriptor file.

Process Compliance

T   F   N/A   1.   The segment has been registered with DISA.

T   F   N/A   2.   The segment has been submitted to and accepted for inclusion in the on-line library.

T   F   N/A   3.   The `VERSION` descriptor has been updated from the previous release in accordance with the requirements specified in Chapter 5. (This does not apply to the initial release of the segment.)

T   F   N/A   4.   The segment is submitted with an annotated output from `VerifySeg`. All warnings are explained in full in `VSOutput`.

T F   N/A   5.   The segment is submitted with a set of integration notes (`IntgNotes`) as described in Chapter 5.

T F   N/A   6.   The `PostInstall`, `PreInstall`, and `DEINSTALL` scripts have been checked and verified to *not* do a Unix `mv` across file partitions.

T F   N/A   7.   The segment has been loaded and tested in the COE environment prior to submission to DISA.

T F   N/A   8.   Segment installation has been tested through the same installation tools used by site operators. (`TestInstall` alone does *not* satisfy this requirement.)

T F   N/A   9.   If removable, the segment has been tested and confirmed that it can be successfully removed from the system.

T F   N/A   10.   If not a permanent segment, the `DEINSTALL` script and `Comm.deinstall` descriptor have been fully tested.

T F   N/A   11.   The segment `Community` descriptor has been fully tested.

Miscellaneous

T F   N/A   1.   The segment creates and initializes dynamic data files that are updated as the system executes (e.g., message logs, operator preferences), or generates a runtime error message if an expected file is missing, and gracefully terminates with an appropriate message to the operator.

T F   N/A   2.   If a patch segment, it follows the patch segment naming convention.

T F   N/A   3.   Prior approval for background and boot processes has been given by the DISA Chief Engineer.

T F   N/A   4.   The segment does not create copies of executables from other segments.

T   F   N/A   5.   The segment does not contain any circular dependencies (e.g., Seg A depends on Seg B, Seg B depends on Seg C, Seg C depends on Seg A is not allowed).

T   F   N/A   6.   The segment does not delete itself during `DEINSTALL`, nor perform any other operations that are handled by the COE installation tools.

B.6 Intermediate COE Compliance (Level 6)

Security

T F   N/A   1.   The segment does not contain any files directly
                             underneath the segment's home directory.

T F   N/A   2.   Classified data is packaged in its own separate
                             segment.

Standards Compliance

T F   N/A   1.   The segment is either completely compatible with the
                             Style Guide, or has minimal deviations that have been
                             approved by the DISA Chief Engineer.

T F   N/A   2.   The segment is available on all COE-supported
                             platforms unless otherwise approved by the DISA
                             Chief Engineer.

T F   N/A   3.   The segment does not alter any community files
                             except through COE segment descriptors or
                             published APIs.

T F   N/A   4.   The segment does not use directories with different
                             names than specified in Chapter 5 to fulfill the
                             purpose of `Scripts`, `bin`, `data`, etc. (`progs` and
                             `libs` are acceptable for this level for as long as the
                             COE tools support them.)

T F   N/A   5.   If the segment contains APIs written in C, the header
                             files for the public APIs are ANSI-C compliant and
                             use function prototypes.

Windowing Environment

T F   N/A   1.   The segment does not alter any X or Motif supplied
                             files (e.g., `Xdefaults`, `rgb.txt`).

Database

T F   N/A   1.   All constraints and business rules are in the database,
                             not the applications.

T F   N/A   2.   Oracle Public Synonyms are not used.

T F   N/A   3.   Database segments do not create user accounts.

T F   N/A   4.   Grants are made to database roles/groups, not user accounts.

T F   N/A   5.   The application does not assume the existence of any particular user.

T F   N/A   6.   Data elements do not use machine dependent data types.

T F   N/A   7.   The segment does not modify another segment's databases except through documented inter-database dependencies.

T F   N/A   8.   The server segment `DEINSTALL` tests for inter-database dependencies.

COTS Products

T F   N/A   1.   All COTS products are packaged as separate, individual COTS segments.

T F   N/A   2.   If a COTS segment, the `PostInstall` script ensures that there is enough space in the directories where the COTS product will be installed and uses `COEInstError` to report an error message if not.

T F   N/A   3.   If a COTS segment, the `FilesList` descriptor has been validated as correctly documenting what files and directories constitute the COTS product. This does not apply to COTS products in the bootstrap COE.

Runtime Environment

T F   N/A   1.   The segment deletes temporary files in the directory pointed to by `TMPDIR` when finished with the files.

T F   N/A   2.   The segment uses relative pathnames for symbolic links used to reference files within the segment.

T F   N/A   3.   The segment, if it uses absolute pathnames to reference files outside the segment, is able to

			determine the absolute path at install time and is able to handle symbolic links to files which are themselves symbolic links.
T	**F**	**N/A**	4. The segment reuses environment variables already defined by the COE or by the affected account group. It does not create any environment variables that are identical in value to those defined by the COE or the affected account group, or that can be derived from them.
T	**F**	**N/A**	5. All global environment settings are established through files in the segment's `Scripts` subdirectory.
T	**F**	**N/A**	6. fonts and app-defaults located underneath the segment's `data` subdirectory are named using the segment prefix.
T	**F**	**N/A**	7. The segment appends, not pre-pends, its `bin` subdirectory to the `path` environment variable.

Segment Descriptors

T	**F**	**N/A**	1. The `ReleaseNotes` descriptor conforms to the requirements stipulated in Chapter 5.

Process Compliance

T	**F**	**N/A**	1. The segment includes an API test suite which exhaustively exercises all APIs provided by the segment.
T	**F**	**N/A**	2. The segment includes man pages for distribution with the Developer's Toolkit.
T	**F**	**N/A**	3. The segment has been compiled without the debug option enabled and has been run through the Unix `strip` program.
T	**F**	**N/A**	4. If the segment has public APIs implemented as shared libraries, static libraries are provided as well.
T	**F**	**N/A**	5. If the segment uses another segment's public APIs and they are implemented as shared libraries, the

segment is submitted linked with the shared libraries and not the static libraries.

T F   N/A   6.   If the segment has a `DEINSTALL` and `Community` descriptor, it also includes a `Comm.deinstall` descriptor which reverses the actions of the `Community` descriptor during segment removal.

T F   N/A   7.   The `DEINSTALL` script has been fully tested.

T F   N/A   8.   The segment has been tested to ensure that it successfully installs over and replaces any previous version of the segment.

T F   N/A   9.   If the segment contains a large static database, it is provided as a separate data segment.

Miscellaneous

T F   N/A   1.   Unless an account group segment, the segment is integrated within one of the predefined account groups.

T F   N/A   2.   If the COE provides functions required by the segment, at least 50% of the functions required are provided by the COE and not by duplicative code in the segment.

T F   N/A   3.   API backwards compatibility conforms to the version numbering scheme described in Chapter 3.

T F   N/A   4.   The segment does not provide access to a command line prompt, except with prior DISA Chief Engineer approval.

T F   N/A   5.   Termination of segment execution, whether premature, inadvertent, or intentional does not place the operator at a Unix level command line prompt.

B.7 Interoperable Compliance (Level 7)

Security

T F   N/A   1.   The segment does not place any temporary files in the directory pointed to by TMPDIR that are sensitive to alteration, deletion, or disclosure to unauthorized users.

T F   N/A   2.   Entering a command line mode requires the operator to enter a password. Mode entry forces execution of the system login process.

T F   N/A   3.   The segment does not contain features with multiple security levels, unless an aggregate segment.

T F   N/A   4.   Unclassified sample data is provided with the segment to allow DISA to conduct unclassified testing and training.

Standards Compliance

T F   N/A   1.   If written in C, the segment is ANSI-C compliant.

T F   N/A   2.   If the segment contains public APIs, Ada and C interfaces are both provided unless a waiver is granted by the DISA Chief Engineer.

T F   N/A   3.   Global and local data owned by the segment are located underneath /h/data as described in Chapter 5.

T F   N/A   4.   Operator specific data is located underneath /h/USERS as described in Chapter 5.

T F   N/A   5.   Excepting COTS segments, all environment variables are named with the segment prefix unless approved by the DISA Chief Engineer. (The Chief Engineer may authorize "grandfathering" of certain environment variables.)

Windowing Environment

T   F   N/A   1.   The segment uses resource files to control window behavior rather than hardcoded window behavior attributes.

Database

T   F   N/A   1   Data objects within the segment do not duplicate those already contained in the corporate database.

T   F   N/A   2.   Database fragmentation schemas are contained in separate segments.

T   F   N/A   3.   Database roles/groups are specific to application privileges, not general purpose.

Runtime Environment

T   F   N/A   1.   The segment does not include any environment variables that could be derived from an already defined environment variable.

T   F   N/A   2.   Segment references to global and local data are done through the DATA_DIR environment variable.

Miscellaneous

T   F   N/A   1.   The segment does not duplicate any functions provided by COE component segments unless approved by the DISA Chief Engineer.

T   F   N/A   2.   No more than 25% of the segment's accesses to COE component segments is through private APIs.

T   F   N/A   3.   If data created or maintained by the segment duplicates data available from the COE or COE-based target system, the amount duplicated by the segment is less than 25%.

B.8 Full COE Compliance (Level 8)

Security

T F N/A   1.   Entry to and exit from the command line mode is audited.

T F N/A   2.   Information written to the audit log includes the segment prefix.

T F N/A   3.   The segment does not mix restricted and unrestricted data files in the same directory.

Standards Compliance

T F N/A   1.   The segment is fully compliant with the *Style Guide*.

T F N/A   2.   The segment does not use any conventions obsoleted by this document (use of `progs` vs. `bin`, use of `COMPONENT` vs. `CHILD`, use of `ModName` and `SegType` vs. `SegName` etc.).

T F N/A   3.   All public symbols are named using the segment prefix.

T F N/A   4.   All directory and file names begin with an alphanumeric character.

T F N/A   5.   The segment follows the convention that data owned by the segment under `/h/data` is in the form `/h/data/local/segdir/data` and `/h/data/global/segdir/data` where `segdir` is the segment's home directory name.

Database

T F N/A   1.   Data elements are chosen from Joint standards and use the data type and units of measure prescribed in the standard.

T F N/A   2.   A test database is provided together with test procedures to verify correct installation of the database and associated roles, and to verify correct operation of constraints defined in the database.

Runtime Environment

T F   N/A   1.   The segment adds no more than one "home"
                              environment variable to the global environment.

Account Groups

T F   N/A   1.   If an account group, all executables are named with
                              the segment prefix.

Segment Descriptors

T F   N/A   1.   The segment uses `SegInfo` rather than individual
                              segment descriptor files.

Process Compliance

T F   N/A   1.   The segment includes a set of test data for verifying
                              correct segment operation.

Miscellaneous

T F   N/A   1.   The segment does not use any private APIs to access
                              external segments. All accesses are through public
                              APIs.

T F   N/A   2.   Operator data is located through the *Preferences* APIs.

T F   N/A   3.   The current operator profile is obtained through the
                              Preferences APIs.

T F   N/A   4.   The segment does not duplicate functionality
                              provided by any other segment unless approved by
                              the DISA Chief Engineer.

T F   N/A   5.   The segment does not duplicate any data already
                              maintained by the COE or the COE-based target
                              system, unless for performance reasons and as
                              approved by the DISA Chief Engineer.

B.9 Recommended Guidelines

The items contained in the following checklist are not mandatory, but are general guidelines for most segments. They are not considered in establishing the COE compliance level.

T F   N/A   1.   The segment does not use symbolic links.

T F   N/A   2.   The segment does not use boot or background processes. It uses session or transient level processes instead.

T F   N/A   3.   The segment allows comments in ASCII data files. The # character is the standard for single line comments while C style comments (delimited by the /* */ pair) are the standard for all other comments.

T F   N/A   4.   The segment links with X and Motif shared libraries.